



NIST CYBERSECURITY & PRIVACY PROGRAM

EXECUTIVE ORDER ON IMPROVING THE NATION'S CYBERSECURITY

The President's Executive Order on Improving the Nation's Cybersecurity (EO 14028), issued May 12, 2021, charges multiple agencies – including the U.S. Department of Commerce's National Institute of Standards and Technology (NIST) – with enhancing the security of the software supply chain.

Section 4 of the Executive Order (EO) directs the Secretary of Commerce, through NIST, to consult with federal agencies, the private sector, academia, and other stakeholders and to identify or develop standards, tools, best practices, and other guidelines to enhance software supply chain security. The resulting standards and guidelines will be used by other agencies to govern the federal government's procurement of software.

NIST has a longstanding program focused on managing risks to the cyber supply chain, software quality and security, and security development and engineering resources – across research, standards and guidelines, and transition to practice. Resources published by NIST and others will serve as a starting point for assignments under the EO.

STANDARDS AND GUIDELINES

The guidelines will address: critical software, secure software development lifecycle, security measures for the federal government, and requirements for testing software. They are to include:

- ➔ criteria to evaluate software security,
- ➔ criteria to evaluate the security practices of the developers and suppliers themselves, and
- ➔ innovative tools or methods to demonstrate conformance with secure practices.
- ➔ By **November 8, 2021**, NIST is to publish preliminary guidelines, based on stakeholder input and existing documents for enhancing software supply chain security.
- ➔ By **February 6, 2022**, after having consulted heads of agencies, NIST will issue guidance that identifies practices that enhance software supply chain security, including standards, procedures, and criteria.
- ➔ By **May 8, 2022**, NIST will publish additional guidelines, including procedures for periodically reviewing and updating guidelines.

CRITICAL SOFTWARE

Security measures for "critical software" are on an even faster track. NIST is to consult with the National Security Agency (NSA), Office of Management and Budget (OMB), Cybersecurity and Infrastructure Security Agency (CISA), and the Director of National Intelligence (DNI) and:

- ➔ define "critical software" by **June 26, 2021**, and
- ➔ publish guidance outlining security measures for critical software by **July 11, 2021**.
- ➔ NIST's definition of critical software will provide criteria that include level of privilege or access required to function, integration and dependencies with other software, direct access to networking and computing resources, performance of a function critical to trust, and potential for harm if compromised.

ADDITIONAL RESPONSIBILITIES

The EO assigns additional responsibilities to NIST, including:

- ➔ initiating two pilot labeling programs related to secure software development practices and the Internet of Things (IoT) to inform consumers about

the security of their products. NIST will initiate those programs working closely with other government agencies and private and public sector organizations and individuals; and

- publishing guidelines by **July 11, 2021**, after consulting with the NSA, recommending minimum standards for vendors' testing of their software source code, including identifying recommended types of manual or automated testing (such as code review tools, static and dynamic analysis, software composition tools, and penetration testing).

WORKSHOP

To ensure robust stakeholder participation in developing standards and guidelines to be produced by NIST, a workshop will be held June 2-3, 2021. At that workshop, NIST will share details about its plans to develop software-related standards and guidelines called for by the EO and receive and discuss information and ideas about the approach and content that NIST should consider in developing those standards and guidelines.

The agenda for the two-day workshop will be based on submissions to NIST by the private, public, and non-profit

sectors in the form of two-page position papers. NIST has published a list of the many resources from which to draw in selecting approaches to improve software security. NIST and non-NIST resources are available here.

NIST CYBERSECURITY FUNDAMENTALS

- ✓ **OPEN AND TRANSPARENT:** NIST's processes bring together stakeholders in an open forum.
- ✓ **COLLABORATIVE:** NIST provides a space for government agencies, businesses, and academic institutions to collaborate.
- ✓ **PRACTICAL:** NIST helps develop practical example solutions to address real-world challenges.
- ✓ **FORWARD-THINKING:** NIST looks to the future and anticipates challenges that lie ahead.

More information about this work is available on a dedicated website.

Information about NIST's broader portfolio of work in cybersecurity and privacy can be found here.

Questions should be directed to: swsupplychain-eo@nist.gov